DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 10 - Contingency Plans

1. References:

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. AR 380-67, Personnel Security Program, 9 September 1988.

   d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   e. DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003.

   f. DoD Instruction 5200.4, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

   g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

   h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

   i. DA PAM 25-1-1, Installation Information Services, 27 August 1991.

2. Purpose: 4ID G6 personnel must be prepared to sustain the automated information systems (AIS) infrastructure in the event of an unexpected disaster, civil disturbance, emergency exercise, mobilization, or war. One of the keys to effective mobilization or recovery is the ability to provide command and control for the influx of troops into active duty, and to provide resiliency of information systems support in the event of a disaster or other emergency event. This policy mandates the development and review of a Disaster Recovery Plan also known as a Continuity of Operations Plan (COOP) that details contingency plans in preparation for the unexpected.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

   a. Commanders, directors, and supervisors at all levels will ensure that subordinate personnel cooperate in the development, maintenance, and awareness of 4ID IA contingency plans.

   b. The 4ID shall be responsible for developing and maintaining operational contingency plans.

5. Policy:

   a. 4ID G6 shall develop and maintain a Continuity of Operations Plan for 4ID AIS. The plan shall be developed in accordance with AR 380-19, Information Systems Security. The plan must address the following:

(1) Risk Evaluation and Control: A risk assessment shall be conducted and updated annually. The risk assessment shall be coordinated with ACERT to perform a CDAP scan on all network devices to identify operating system vulnerabilities and ensure that the devices are configured to manage risks to the AIS infrastructure. Determine the events and environmental surroundings that can adversely affect the post and its facilities with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Critical operations and supporting infrastructure shall be identified and the value of the operation quantified to the extent practicable. The maximum downtime that can be tolerated before unrecoverable loss can be expected shall be calculated for each critical operation. The frequency of anticipated losses shall be calculated for each type of loss factored into the risk assessment. A cost-benefit analysis to justify investment in controls to mitigate risks shall be developed.

(2) Business Impact Analysis: The cost of AIS assets shall be quantified and the annual loss expectancy calculated. Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Through this process 4ID EOM will identify critical organizational functions, their criticality and recovery priorities, and interdependencies so that the recovery time objective (RTO) can be set. The business impact from recommended enhancements to minimize risks shall be quantified. The anticipated loss expectancy from each realistic disaster or contingency shall be estimated. The RTO shall be estimated so that recovery occurs before unrecoverable losses begin to accumulate.

(3) Developing and Implementing Continuity of Operations Plans: Determine the alternative business recovery operating strategies for recovery of operations and information technology resources within the RTO, while maintaining the organizations critical functions. Design, develop, and implement COOP plans that provide recovery within the RTO.

(4) Emergency Response and Operations: Develop and implement procedures for response and stabilizing situations including establishing and managing an Emergency Operations Center to be used as a command and control center during the emergency.

(5) Awareness and Training Programs: Prepare a program to create organizational awareness and enhance the skills required to develop, implement, maintain, and execute the COOP plan. Communication of the plan to participants is a key to its success.

(6) Maintaining and Exercising the Continuity of Operations Plan: The 4ID EOM and IAM will pre-plan and coordinate a COOP exercise, and evaluate and document the plan exercise results. The 4ID EOM will develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the 4ID's strategic direction. The IAPM will then certify to the 4IDG6 that the Plan remains current.

(7) Public Relations and Crisis Communications: The 4ID EOM will develop, coordinate, evaluate, and exercise plans to handle media during crisis situations. The IAM will assist the 4ID EOM to develop coordinate, evaluate, and exercise plans to communicate with and, as appropriate, provide trauma counseling for employees and their families, key customers (agencies or Commands), critical suppliers, and senior management during the crisis. The 4ID EOM and IAM will develop a plan to ensure that all stakeholders are kept informed on an as-needed basis.

(8) Coordination with Public Authorities: The IAM will work with 4ID EOM to establish applicable procedures and policies for coordinating response, continuity, and restoration activities with local authorities while ensuring compliance with applicable statutes or regulations.

b. Assistance in the development of Continuity of Operations Plans may be obtained from the IAM.

c. The 4ID IAM shall review the COOP plans of 4ID EOM on an annual basis to ensure the plans are current. The IAM shall report the status of contingency preparedness to the 4ID annually.

d. 4ID EOM shall develop and participate in a COOP exercise on a bi-annual basis.

e. The IAM will assist 4ID EOM in evaluating the effectiveness of contingency plan exercises.

6. Non-Compliance:

The Director, 4ID EOM will be held accountable for the development and exercise of Continuity of Operations Plans under their operational oversight in accordance with this policy. Failure to develop or properly maintain a Continuity of Operations Plan places 4ID IA operational readiness at risk. The development of a successful COOP plan requires cooperative efforts by many affected parties. Failure to support the development and exercise of a COOP plan shall be reported to the 4IED EOM through the IAPM for further action as deemed appropriate.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding

DISTRIBUTION:
4ID
Organizations Attached to 4ID Networks.